Proposal Topic

BitCoin Exchange Trust Network Analysis

Shiv Raj Pant, Xiaoqin Fu

School of Electrical Engineering and Computer Science

Washington State University

Pullman, WA

Email: {shiv.pant, xiaoqin.fu}@wsu.edu

I. Introduction

BitCoin was developed in 2008 and 2009 as a radical new concept for money and currency [1] using blockchain technology. Our research focuses on study data from a BITCOIN marketplace with interactions and ratings [2]. They are (directed) weighted signed network (WSN) in which edge corresponds to some weight, the rating from user u to user v [3]. They forms webs of trust between users allowing two unknown users to perform a transaction based on the aggregated trust [3].

II. Methodology

Our paper is to study the two trust networks: Bitcoin OTC web of trust network and Bitcoin Alpha web of trust network, and analyze the relationship between price and trust. Moveover, we will predict edge weights from time stamp data in the data sets. For the experiment, we will extract both topological and non-topological features from the networks [4] [5] [6].

III. Data

We will use two data sets, soc-sign-bitcoin-otc and soc-sign-bitcoin-alpha, from [7]. OTC and Alpha are two Bitcoin exchanges, which are open market websites allowing users to buy and sell things [7]. The soc-sign-bitcoin-otc, Bitcoin OTC web of trust network, is a (directed) weighted signed network (WSN) with 5,881 nodes and 35,592 edges. On Bitcoin OTC, people can build up trust to exchange bitcoins with ratings from -10 (total distrust) to 10 (total trust) which are associated with how much a user trusts another user [3]. A high rating is mapping the high trust. The data set has the rating times recorded as seconds since Epoch [7].

And the soc-sign-bitcoin-alpha, Bitcoin Alpha web of trust network, is also a directed WSN with 3,783 nodes and 24,186 edges. It is similar in almost every way to the soc-sign-bitcoin-otc. It also has ratings from -10 to 10 and the rating times. While the OTC network is still active, the Alpha exchange is no longer active now [3].

IV. Related work

A. Blockchain

Blockchain is a distributed database which keeps record in a distributed fashion. Figure **??** shows the schematic diagram of blockchain. A block encrypts the data using cryptographic hash function, such as SHA-256, and keeps record of next available block for traversing the blocks. Records are stored in a tree structure where the leaves stores the transaction information and other intermediate nodes store the hash values. The root of this tree belongs in a block containing the hash value generated from child nodes. The timestamp in a block is used to synchronize the position of a block in blockchain. A block also contains NONCE value, which is random unique number for a specific block.

B. Proof–of–Work

Proof–of–work (POW) method was invented by Cynthia Dwork and Moni Naor back in 1993. The term proof–of–work was coined by Markus Jakobsson and Ari Juels in a document published in 1999. In order to secure the transaction in a distributed database like block chain, Satoshi Nakamoto adopted this method in blockchain network.

This method deals with two parties, one is miner and the other one is verifier. Miners mine inside a block to find all the transactions belongs in that block. After mining all the transactions of a block that block is ready to add in the public blockchain and verifier can easily verify the transaction request. When a miner solves a block, it gains some reward in form of bitcoin.

C. Proof–of–Stake

Proof–of–Stake (POS) is an alternate method of Proof–of–Work described above. A miner or verifier can validate a block based on the amount of stake that verifier holds. The more stake a miner holds, the more mining power gained.

D. IOTA Network

IOTA is an alternate of Bitcoin and it used Tangle as a distributed ledger instead of Blockchain. Fig. 1 shows the structure of the tangle network. The network is a directed acyclic graph where each node indicates an entity that issue and validate transaction [8]. The edge indicates the relationship between a new transaction and the old transaction. The direction of an edge is from a new transaction to one of the recent transactions. In order to approve a new transaction, tangle verify most recent two transactions, hence, each node points to at most two previous nodes in terms of time.

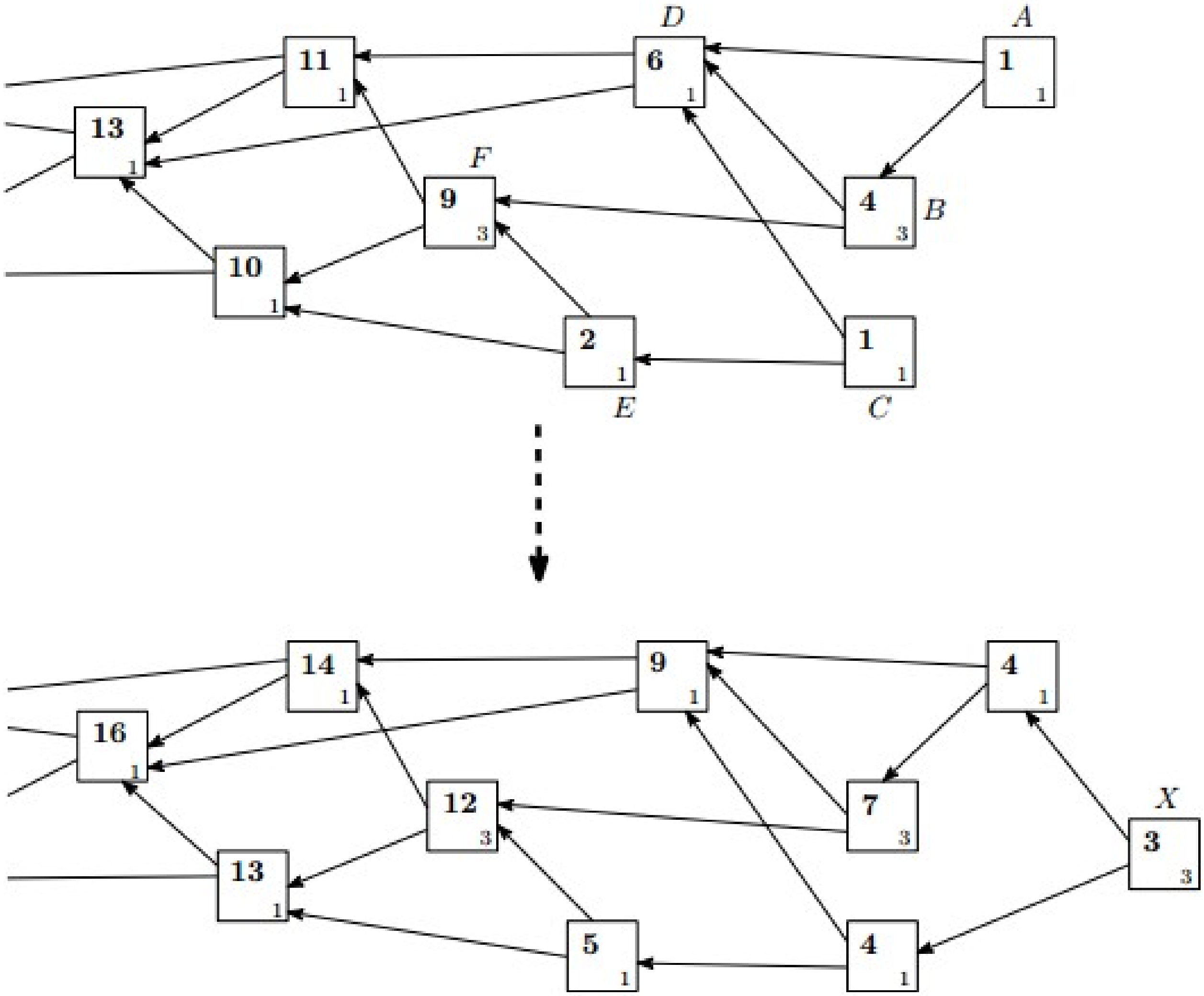

Fig. 1: The network achitecture of tangle. Each node is an entity that issue and validate transaction. The nodes are growing from left to right accoring to the grow of time. This figure regenerated from [8].

Each node contains information of two weights , one is its own weight (right–botton corner) and the another one is the cummulative weight (at center). The cummulative weight of a node is the summation of all the node weights alongs the path that ends at that node. According to Fig. 1, the nodes of all the paths those ended at node F are A,B,C and E. The cumulative weight of F is $\sum_{s\in\{A,B,C,D,F\}} \omega(s) = 1+3+1+1+3 = 9$. The weight feature prevent tangle from a quantum computer attack [8].

V. Tentative plan

-
-
-
-

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[2] E. H. Aw, R. Gera, K. Hicks, N. Koeppen, and C. Teska, "Analyzing preferential attachment in peer-to-peer bitcoin networks," in *2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*. IEEE, 2018, pp. 1242–1249.

[3] O. Moindrot, "Trust in bitcoin exchange networks," 2017.

[4] D. Liben-Nowell and J. Kleinberg, "The link-prediction problem for social networks," *Journal of the American society for information science and technology*, vol. 58, no. 7, pp. 1019–1031, 2007.

[5] M. Al Hasan, V. Chaoji, S. Salem, and M. Zaki, "Link prediction using supervised learning," in *SDM06: workshop on link analysis, counter-terrorism and security*, 2006.

[6] D. Davis, R. Lichtenwalter, and N. V. Chawla, "Multi-relational link prediction in heterogeneous information networks," in *2011 International Conference on Advances in Social Networks Analysis and Mining*. IEEE, 2011, pp. 281–288.

[7] J. Leskovec and A. Krevl, "SNAP Datasets: Stanford large network dataset collection," http://snap.stanford.edu/data, Jun. 2014.

[8] S. Popov, "The tangle," *cit. on*, p. 131, 2016.